Leçon 122 : Anneaux principaux. Applications.

Rombaldi

Ulmer Anneaux, ... (dev 1 & 2)

Dans cette leçon, A désigne un anneau commutatif unitaire.

I - La notion de principalité

1. Définition et premières propriétés

Définition 1.1 Un idéal I de A est dit principal s'il existe $a \in A$ tel que $I = (a)$.

Définition 1.2 On dit que A est un anneau principal si A est intègre et si tout idéal de A est principal.

Exemples 1.3

- un corps est un anneau principal : ses seuls idéaux sont (0) et (1)
- $\mathbb{Z}$ est un anneau principal
- $\mathbb{Z}[X]$ n'est pas un anneau principal car $(2, X)$ n'est pas un idéal principal

Proposition 1.4 Soient A un anneau principal et $p \in A \setminus A^*$. Alors les assertions suivantes sont équivalentes :

- (p) est premier
- p est irréductible
- p est premier
- (p) est maximal

2. Un cas particulier : les anneaux euclidiens

Définition 1.5 On dit que A est euclidien si A est intègre et s'il existe un stathme φ tel que pour tous $a, b \in A$ avec $b \neq 0$, il existe un couple $(q, r) \in A^2$ tel que l'on ait $a = bq + R$ avec $R = 0$ ou $a \neq 0$ et $\varphi(a) < \varphi(b)$.

Exemple 1.6

$\mathbb{Z}$ est un anneau euclidien

Proposition 1.7 Un anneau euclidien est principal.

Contre - exemple 1.8 (admis)

L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est un anneau principal non euclidien.

3. Un exemple important : $\mathbb{K}[X]$

Lemme 1.9 Soit $P \in A[X]$ non nul de coefficient dominant inversible. Soit $F \in A[X]$, il existe alors $Q, R \in A[X]$ tels que $F = PQ + R$ avec $R = 0$ ou $\deg R < \deg P$.

Conséquence 1.10 Si $\mathbb{K}$ est un corps alors $\mathbb{K}[X]$ est euclidien donc principal.

Proposition 1.11 Il y a équivalence entre les assertions suivantes :

(i) $A[X]$ est principal

(ii) $A[X]$ est euclidien

(iii) A est un corps

II. Arithmétique dans les anneaux principaux

1. Généralités

Théorème 2.1 Supposons que A soit un anneau principal. Soient $a_1, \dots, a_r \in A^*$, avec $r \geq 2$, il existe alors $d \in A^*$ tel que $(a_1, \dots, a_r) = (d)$ et cet élément s'écrit $d = \sum_{k=1}^{r} u_k a_k$ avec $u_1, \dots, u_r \in A$.

L'élément d est un pgcd de $a_1, \dots, a_r$.

Définition 2.2 Soient $r \geq 2$ et $a_1, \dots, a_r \in A$ principal. On dit que $a_1, \dots, a_r$ sont premiers entre eux dans leur ensemble si leur pgcd est dans A^*.

Théorème 2.3 (Gauss) Deux éléments a, b de A principal sont premiers entre eux si et seulement si pour tout $c \in A$, a divise bc implique a divise c.

Théorème 2.4 (Bézout) Des éléments $a_1, \dots, a_r$ tous non nuls de A principal sont premiers entre eux dans leur ensemble si et seulement s'il existe $u_1, \dots, u_r \in A$ tels que $\sum_{k=1}^{r} u_k a_k = 1$.

Théorème 2.5 Soient $a_1, \dots, a_r$ éléments tous non nuls de A principal. Il existe $m \in A$ tel que $\bigcap_{k=1}^{r} (a_k) = (m)$ et m est ppcm de $a_1, \dots, a_r$.

Corollaire 2.6 Soient $a_1, \dots, a_r \in A$ principal. Si les a_k sont deux à deux premiers entre eux alors $\text{ppcm}(a_1, \dots, a_r) = \prod_{k=1}^{r} a_k$ à un inversible près.

2. Le théorème chinois

Théorème 2.7 Soient $a_1, \dots, a_r \in A$ premiers entre eux deux à deux avec A principal. Alors l'application $\varphi : x \in A \longmapsto (\pi_j(x))_j \in \bigotimes_{k=1}^{r} A/(a_k)$ est un morphisme d'anneaux surjectif. Il induit un isomorphisme $\overline{\varphi} : A/(a) \longrightarrow \bigotimes A/(a_k)$ où $a = \prod_{k=1}^{r} a_k$, d'inverse $\overline{\varphi}^{-1} : (\pi_j(x_j))_j \longmapsto \sum_{i=1}^{r} x_i u_i b_i$ où $b_i = \prod_{k \neq i} a_k$ et $\sum_{j=1}^{r} u_j b_j = 1$.

développement 1

Application 2.8
Résolution du système $\begin{cases} f(\bar{0}) = \bar{2} \\ f(\bar{1}) = \bar{0} \\ f(\bar{2}) = \bar{1} \end{cases}$ dans $\mathbb{Z}_5[X]$

Application 2.9
Résolution du système $\begin{cases} u \equiv 1 \pmod 3 \\ u \equiv 3 \pmod 5 \\ u \equiv 0 \pmod 7 \end{cases}$ dans $\mathbb{Z}$

III - Applications ...

1. ... à l'algèbre linéaire

Soient $\mathbb{K}$ un corps (commutatif), E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathcal{L}(E)$.

Lemme 3.1 (des noyaux) Soit $P = P_1^{\alpha_1} \dots P_r^{\alpha_r} \in \mathbb{K}[X]$ où les P_k sont irréductibles deux à deux distincts. Alors $\ker P(u) = \bigoplus_{k=1}^{r} \ker P_k^{\alpha_k}(u)$.

Définition 3.2 Soit $I = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$. Alors I est un idéal de $\mathbb{K}[X]$, non réduit à $\{0\}$. On appelle polynôme minimal, le polynôme π_u vérifiant $I = (\pi_u)$.

Proposition 3.3 L'endomorphisme u est diagonalisable si et seulement si π_u est scindé à racines simples dans $\mathbb{K}$.

2. ... à la résolution d'une équation diophantienne

Définition 3.4 On appelle anneau des entiers de Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

Proposition 3.5 L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $a + ib \longmapsto |a + ib|^2 = a^2 + b^2$.

On note $\Sigma_2 = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N};\ n = a^2 + b^2\}$.

Lemme 3.6 Soit $n \in \Sigma_2$ alors $n \equiv 0, 1, 2 \pmod 4$. Dans le cas particulier où n est impair, $n \equiv 1 \pmod 4$.

Théorème 3.7 (Fermat) Soit p un nombre premier. Alors $p \in \Sigma_2$ si et seulement si $p \equiv 1 \pmod 4$.

développement 2